VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA", BELGAUM – 590018

A

Project Report on

"EFFICIENT IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGYAPHY ON DSP"

(Sponsored by KSCST,Banglore)

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF ENGINEERING IN ELECTRONICS & COMMUNICATION ENGINEERING

Submitted By

Mr. Rohit P. More	**USN: 2JI10EC034**
Ms. Urmila V.Dhavali	**USN: 2JI10EC048**
Ms. Zuhi M. Subedar	**USN: 2JI10EC051**

Under the Guidance of

GUIDE	CO-GUIDE
Prof. Rajashree Khanai	**Prof. Niranjan Muchandi**

JAIN COLLEGE OF ENGINEERING, BELGAUM

2013-14

ABSTRACT

This project studies the mathematics of elliptic curves, starting with the understanding of how points upon the curves form an additive abelian group. We then work on the mathematics necessary to use these groups for cryptographic purposes, specifically results for the group formed by an elliptic curve over a finite field, E(Fq). We examine the mathematics behind this elliptic curves and then use the results for formulating a code that encrypts and decrypts the data successfully along with a number of other useful results. We finish by implementing the algorithm by dumping it on DSP(TMS320C6713) and showing how this can form public key cryptographic systems for use in both encryption and key exchange.